

# AFOTEC hosts Easter Egg Hunt



*Above:* The Easter Bunny’s helper, Jeanie Tovrea, offers goodies to one guest.

*Below:* Mike McHugh helps one guest hit the pinata target.



The Easter Bash was held April 16 at Bicentennial Park. About 60 children of Air Force Operational Test and Evaluation personnel were treated to games, special treats and an Easter egg hunt. Jeanie Tovrea was this year’s Easter Bunny. The Easter Bash is one of several special youth-oriented events that AFOTEC sponsors each year for family members.



Photos by Todd Berenger



*Above:* Children get ready for the egg race.

*Left:* This young guest expresses his victory finding East eggs at the Air Force Operational Test and Evaluation Centers’ Easter Bash egg hunt.

*Below:* Easter Bash goers gather goodies from the pinata.



*Left:* Maj. Shawn Smith practices his face-painting skills with a youngster at the Air Force Operational Test and Evaluation Center’s Easter Bash.

*Below:* Even the youngest Easter Bash guests enjoyed the egg hunt.





# New identification cards are secure, ready

**AIR FORCE PERSONNEL CENTER** - The high-tech identification Common Access Card, or CAC, currently replacing familiar green IDs worldwide is secure and proven in combat, despite some rumors to the contrary.

“Worries are unfounded” that the new IDs are easily accessible to identity thieves or even hostile forces, said Chief Master Sgt. Ricky Arnold, Survival, Evasion, Resistance, and Escape program manager at the Pentagon.

“These cards are not a risk to anyone’s privacy or security,” said the chief. “We thoroughly researched the security risks before we even began to issue common access cards,” said Maj. Gen. Richard Mentemeyer, director of operations and training at the Air Staff.

“We were satisfied then, and recent events have reinforced our belief that common access cards are not only secure and safe but also provide required Geneva Conventions information in the event an Airman is captured,” the general said.

“In a war zone or at home station, there should be no hesitation: Don’t leave home without it,” he said.

The card does not contain any personal information electronically that isn’t already printed on the card, officials said. What it does is allow for electronic access to computer systems that contain personal data. Also, an extra layer of protection is provided when a card is reported lost or the cardholder goes into missing or captured status. At that point computer and data system access is turned off, officials said.

And built-in electronic security measures make getting access to what information is on the chip extremely difficult, if not impossible, officials said.

“To date, there has not been a single successful attempt to extract information from one of these cards. We know that Airmen isolated in hostile areas don’t have to worry, because we have tested and validated during Operation Iraqi Freedom the process for turning off computer access,” Chief Arnold said.

Common access cards should be issued across the Department of Defense by October to all eligible Air Force active duty, guard, reserve, civilians and some contractors, officials said.

Rumors that some deployed Airmen destroyed or lost their CAC cards in an effort to



Photo by Master Sgt. Jon Niccolussi

## Romanian students get the New Mexico ‘red or green’ question, football coaching

**TEAM KIRTLAND**Der 1st. Lt. Kelley Jeter of the 377th Air Base Wing Public Affairs office talks to a Romanian student about New Mexico. Joining her are Jeter’s Romanian counterpart, Capt. Florin Sperle (left) and Maj. Tony Thomas, her communications commander (right). Fifteen members visited a Romanian school as part of a community relations project. During the visit, the military members attempted sharing American football, but the students reverted each time to playing rugby.

get an old-fashioned green ID card reissued to them spurred officials to conduct an informal study into the matter, the chief said.

“The results showed no evidence of that sort of activity—which would be illegal, since the cards are government property,” he said.

“The statistics don’t show any cases where people are intentionally maneuvering to get old-style cards. And we checked specifically for indications of that. It just seems to be a completely unfounded rumor,” he said.

Even in hostile areas, the new CACs do not

put peoples’ privacy and security at risk, officials said.

Each card bears a color photo and service seal of the holder, required visible personal data, a magnetic strip, linear and two-dimensional barcodes, and a 32 kilo-byte computer chip.

Even if someone had the extensive knowledge and expensive equipment needed to get information off the chip, an attempt would take longer than eight hours per card, and cause the card to be deactivated and/or destroyed in the process, he said.